

SECURINETS



**CLUB DE LA SECURITE INFORMATIQUE
INSAT**

SECURILIGHT 2011

Crack Mot de passe Linux

Chef Atelier : Asma Touihri (RT2)

Rania Touihri (MPI)

Yosra Ghazoueni (RT3)

Insaf bejaoui (RT3)

Rim msalmi (MPI)

30/11/2011

I. Introduction :

Password Cracking ou le cassage de mot de passe est un procédé de recouvrement de mot de passe ou d'une clé d'un système informatique pour y accéder.

Ce procédé a pour but d'aider un utilisateur à retrouver un mot de passe perdu ou d'obtenir un accès non autorisé au système. Sur le plan professionnel, ce processus représente une mesure préventive permettant de vérifier le niveau de sécurité réel des mots de passe (ou leur fiabilité) .

A travers ce tutoriel, nous allons utiliser le logiciel John The Ripper pour trouver le(s) mot(s) de passe sous linux, sans l'installer.

II. John The Ripper : Présentation et explications

John The ripper (JTR) est un logiciel libre de cassage de mot de passe qui a été développé par Alexander Peslyak. Ce logiciel est capable de casser différents formats de chiffrement de mot de passe, notamment les mots de passe crypt, MD5 ,Blowfish ,AFS ...

La fonction de John est de tester toutes les combinaisons possibles en commençant par les plus probables, soit d'une liste de mot, soit de manière incrémentale pour faire correspondre le hash du mot de passe crypté avec celui du mot testé.

Vous n'aurez pas nécessairement besoin d'installer **John the Ripper**, en effet, il vous suffira de télécharger dans votre PC, le fichier de démarrage et vous pourrez commencer à l'utiliser sans aucun problème. Voyons comment procéder !

1. Allez sur la page <http://www.openwall.com/john/> et téléchargez la version que vous désirez.

2. N'oubliez pas que JTR s'exécute en lignes de commande, alors ouvrez votre terminal (Applications > Accessoires > Terminal).

3. En utilisant les commandes, accédez à votre dossier de JTR (là ou vous l'avez enregistré). Dans mon cas, je l'ai enregistré sur le bureau.

```
rania@rt-virtual-machine:~$ sudo su
root@rt-virtual-machine:/home/rania# cd Bureau
root@rt-virtual-machine:/home/rania/Bureau# cd john-1.7.3.1
```

4. Maintenant, accédez au dossier "run" puis entrez cette commande : ". /john /etc/shadow " qui vous permettra d'accéder au fichier "shadow". En effet, c'est ce fichier là qui contient tous vos mots de passe (cryptés) enregistrés sur votre machine.

```
root@rt-virtual-machine:/home/rania/Bureau/john-1.7.3.1# cd run
root@rt-virtual-machine:/home/rania/Bureau/john-1.7.3.1/run# ./john /etc/shadow
Loaded 2 password hashes with 2 different salts (generic crypt(3) [?/32])
```

5. Il vous a indiqué le nombre de mots de passe qu'il a trouvé, dans mon cas 2 ("loaded 2 password hashes ..."). Maintenant, cliquez sur "entrée" pour lancer JTR !

6. Si vous pressez n'importe quelle touche vous verrez apparaître une ligne du type :
" guesses : U time: V W% (X) c/s : Y trying : Z " . Ne vous inquiétez pas c'est facile de
comprendre cette ligne ! En effet:

- "U" : représente le nombre de mots de passe cassés.
- "V" : représente le temps depuis le début de l'attaque.
- "W" : représente le pourcentage effectué dans l'attaque.
- "X" : représente le mode utilisé (simple, dictionnaire, ou incrémental).
- "Y" : représente le nombre de coups par seconde.
- "Z" : représente la dernière chaîne de caractères testée.

7. Cliquez successivement sur une touche pour voir la progression de l'attaque.

```
guesses: 1 time: 0:00:00:04 7% (1) c/s: 24.93 trying: rania6
guesses: 1 time: 0:00:00:06 8% (1) c/s: 25.29 trying: raniah
guesses: 1 time: 0:00:00:11 12% (1) c/s: 25.13 trying: rania99999.
guesses: 1 time: 0:00:00:14 14% (1) c/s: 25.12 trying: Rania1
guesses: 1 time: 0:00:00:34 38% (1) c/s: 24.25 trying: Frania
guesses: 1 time: 0:00:00:53 55% (1) c/s: 22.51 trying: rania9999912
guesses: 1 time: 0:00:01:58 89% (1) c/s: 19.25 trying: r999991980
```

C'est un aperçu du premier mode d'action de JTR à savoir le mode simple , indiqué par le
chiffre (1). Dans ce mode, John effectue quelques transformations sur le nom d'utilisateur
(dans mon cas : Rania) pour casser les mots de passes les plus faibles.

8. Une fois l'attaque est terminée (atteint 100%) sans pour autant trouver le mot de
passe qu'on cherche, JTR passe automatiquement au deuxième mode d'action qui est
l'attaque par dictionnaire indexé par le chiffre (2).

```
guesses: 1 time: 0:00:04:21 1% (2) c/s: 17.14 trying: bucks
guesses: 1 time: 0:00:04:31 1% (2) c/s: 17.05 trying: dianne
guesses: 1 time: 0:00:06:02 3% (2) c/s: 16.55 trying: 0u812
guesses: 1 time: 0:00:08:08 4% (2) c/s: 16.18 trying: Jazz
guesses: 1 time: 0:00:11:18 6% (2) c/s: 15.86 trying: ketchups
```

Dans ce mode, John essaye un à un tous les mots d'une liste de mots de passe potentiels,
(par défaut, password.lst fournie avec contenant plus de 3000 mots) en leur appliquant les
mêmes transformations que dans le mode précédent.

9. Une fois le mot de passe retrouvé , JTR l'affiche directement.

```
guesses: 1 time: 0:00:11:18 6% (2) c/s: 15.86 trying: ketchups
welcome1 (rania)
guesses: 2 time: 0:00:12:16 100% (2) c/s: 15.80 trying: welcome1
```

Dans le cas échéant, JTR effectue son dernier mode d'action qui est le mode incrémental.
Dans ce mode, John va essayer toutes les combinaisons de caractères possibles, jusqu'à
trouver le mot de passe. Tous les caractères étant testés, ce mode est *techniquement*
infaillible, bien que la robustesse du mot de passe influe grandement sur le temps de calcul
nécessaire à le trouver.

III. Prévention et sécurité:

Comme son nom l'indique, dans cette dernière rubrique du tutoriel , on va
s'intéresser à la partie de la protection qui concerne le choix de votre mot de passe.

a. Qu'est-ce qui fait un bon mot de passe?

Un mot de passe fort se compose de :

- ✓ 8 caractères au minimum, de préférence 10 et idéalement 14.
- ✓ des majuscules et des minuscules, des chiffres et des caractères spéciaux mixés ensembles.
- ✓ au moins un caractère spécial entre la deuxième et la sixième position.

Un mot de passe fort ne doit pas contenir :

- X des combinaisons en séquence (123456, 55555 ou klmnop) ou voisines sur le clavier (azerty, qsdffg).
- X les prénoms, les dates et les mots qui se trouvent dans le dictionnaire.
- X vos informations privées.

b. Comment mémoriser un tel mot de passe ?

Quand on lit les instructions à suivre pour avoir un bon mot de passe, on a l'impression que ça ressemble à un vrai casse-tête ! Mais, ne vous inquiétez pas , il existe plusieurs astuces pour mémoriser vos mots de passe complexes! L'une des techniques les plus couramment utilisées s'appuie sur une phrase à mémoriser.

Eh oui ! une simple phrase peut vous aider énormément pour ne pas oublier vos mots de passe ! Prenons l'exemple de cette phrase : " Ce matin, j'ai acheté 3 stylos pour 660 millimes ".

Il suffit alors de prendre la première lettre de chaque mot, en incluant la ponctuation et les chiffres. Vous obtenez alors : " **Cm, j'aa3sp660m** ", un vrai mot de passe fort ! Vous pouvez compliquer la technique en insérant d'autres caractères spéciaux ...

c. Doit-on changer régulièrement ses mots de passe ?

C'est fortement recommandé, au moins deux ou trois fois par an.

d. Est-il raisonnable de noter ses mots de passe quelque part?

Surtout pas! Un bon mot de passe doit être mémorisé jamais écrit !

Cela dit, vous pouvez vous permettre de noter vos mots de passe importants, à condition de ranger le papier dans un endroit sûr , mais évitez de les écrire dans des fichiers de texte.

IV. Conclusion:

Il en va sans dire que l'utilisation de ce type de software de crack devra se faire d'une manière responsable, en l'utilisant à des fins éthiques et dans le but de contrôler la sécurité de vos mots de passe. N'oubliez pas que notre objectif est toujours d'assurer le maximum de protection possible !